

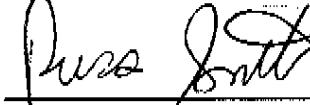
Russ Smith, *pro se*  
PO Box 1860  
Ocean City, NJ 08226  
609-398-3301 (voice/fax)  
[smith@help.org](mailto:smith@help.org)

UNITED STATES DISTRICT COURT  
DISTRICT OF NEW JERSEY

Russ Smith, <i>pro se</i>	:	Civil Action No. 1:09-cv- 04567(RBK)(KMW)
Plaintiff,	:	NOTICE OF MOTION
 v.		
Trusted Universal Standards in Electronic Transactions, Inc. (d/b/a, TRUSTe, Inc.), Microsoft, Inc., Cisco Systems, Inc., and Comcast Cable Communications, LLC	:	
Defendants	:	

---

PLEASE TAKE NOTICE Russ Smith will move before the Honorable Robert B. Kugler U.S.D.J, on November 16, 2009 for leave to file an amended complaint. The Plaintiff's First Amended Complaint is attached. In support of the motion Plaintiff will rely on the attached brief.

  
\_\_\_\_\_  
Russ Smith, *pro se*  
PO Box 1860  
Ocean City, NJ 08226  
609-398-3301 (voice/fax)  
[smith@help.org](mailto:smith@help.org)

Date: October 8, 2009

**Russ Smith, pro se**  
 PO Box 1860  
 Ocean City, NJ 08226  
 609-398-3301 (voice/fax)  
 smith@help.org

**UNITED STATES DISTRICT COURT  
 DISTRICT OF NEW JERSEY**

**Russ Smith, pro se**

Civil Action No. 1:09-cv-  
 04567(RBK)(KMW)

**Plaintiff,**

**PLAINTIFF'S MOTION BRIEF  
 FOR  
 LEAVE TO FILE  
 FIRST AMENDED  
 COMPLAINT**

v.  
 Trusted Universal Standards In  
 Electronic Transactions, Inc. (d/b/a,  
 TRUSTe, Inc.), Microsoft, Inc., Cisco  
 Systems, Inc., and Comcast Cable  
 Communications, LLC

**Defendants**

**Table of Contents**

<b>Summary .....</b>	<b>1</b>
----------------------	----------

**Table of Authorities**

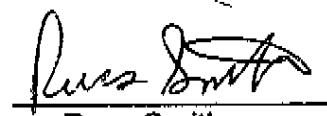
<b>Fed. R. Civ. Pro. 15 .....</b>	<b>1</b>
<b>47 USC Sec. 551 and 47 C.F.R. § 76.1716 .....</b>	<b>2</b>

**Summary**

1. Pursuant to Fed. R. Civ. Pro. 15 Plaintiff seeks to file an amended complaint to:
  - a. Add a count against Microsoft pursuant to the Electronic Communications Privacy Act based on their representation that they collected e-mails sent by Plaintiff,
  - b. Add an issue about Microsoft claiming to Plaintiff, TRUSTe and the court that the Microsoft Frontbridge service privacy policy is not

licensed by TRUSTe. While Microsoft has made representations in public comments to the Federal Trade Commission that TRUSTe licenses all Microsoft Corporation privacy policies,

- c. Add an issue and count relating to TRUSTe making the representation that TRUSTe licenses all of Comcast's privacy policies when TRUSTe actually only licenses some of them,
- d. Add a count concerning Comcast's failure to adhere to 47 USC Sec. 551 and 47 C.F.R. § 76.1716,
- e. Add more than 50 exhibits that identifies applicable contracts known to Plaintiff and clarify other issues,
- f. Specify and clarify compensatory, punitive and statutory damages, and
- g. Correct errors.



Russ Smith, pro se  
PO Box 1860  
Ocean City, NJ 08226  
609-398-3301 (voice/fax)  
smith@help.org

Date: October 8, 2009

**Russ Smith, pro se**  
 PO Box 1860  
 Ocean City, NJ 08226  
 609-398-3301 (voice/fax)  
 smith@help.org

**UNITED STATES DISTRICT COURT  
 DISTRICT OF NEW JERSEY**

**Russ Smith, pro se**

Civil Action No. 1:09-cv-  
 04567(RBK)(KMW)

Plaintiff,

**First Amended  
 Complaint**

v.

**Trusted Universal Standards in  
 Electronic Transactions, Inc. (d/b/a,  
 TRUSTe, Inc.), Microsoft, Inc., Cisco  
 Systems, Inc., and Comcast Cable  
 Communications, LLC**

Defendants

**Table of Contents**

<b>Summary .....</b>	<b>2</b>
<b>Plaintiff .....</b>	<b>5</b>
<b>Defendant TRUSTe .....</b>	<b>8</b>
<b>Defendant Microsoft .....</b>	<b>10</b>
<b>Defendant Comcast .....</b>	<b>13</b>
<b>Defendant Cisco .....</b>	<b>16</b>
<b>Plaintiff's Internet Connection and Email Configuration .....</b>	<b>17</b>
<b>Advice to Internet Industry by FCC and FTC .....</b>	<b>19</b>
<b>Comcast's Policies not Enforceable by Comcast .....</b>	<b>21</b>
<b>Microsoft IP Address Blacklisting of Plaintiff .....</b>	<b>22</b>
<b>Comcast Blocking E-mail Communications of Plaintiff .....</b>	<b>25</b>
<b>Cisco Fraudulently Operating E-mail "Credit" Reporting Service .....</b>	<b>28</b>

Defendants Further Violations of Privacy Policies .....	29
Counts – TRUSTe .....	29
Counts – Comcast .....	31
Counts – Microsoft .....	32
Counts – Cisco .....	34
Relief Sought .....	35

#### Table of Authorities

New Jersey Consumer Fraud Act	<u>N.J.S.A.</u>	56:8-2	<i>et seq.</i> ,
.....	.....	4,5,10,11,13,16,31,34,37	
Electronic Communications Privacy Act [Federal Wiretap act,			
18 U.S.C. § 2510, <i>et seq.</i> and			
Pen Register Act 18 U.S.C. § 2510, <i>et seq.</i> ] .....	4,5,31,33,35,37		
The New Jersey Wiretapping and Electronic Surveillance Control Act, <u>N.J.S.A.</u>			
2A:156A-1 .....	4,6,31,34,37		
47 USC Sec. 551 and 47 C.F.R. § 76.1716.....	4,5,27,29,32,37		
ANSI ISO/IEC Standard 17024:2003 .....	7		
Section 501(c)(6) of the Internal Revenue Code .....	9, 10		
Bell v Acxiom 2006 WL 2850042 (E.D. Ark. Oct 3, 2006) .....	35		

#### Summary

1. Plaintiff asserts that

- a. Defendants Microsoft, Cisco, and Comcast have developed Internet “profiles” of Plaintiff by intercepting Internet communications and other means,

- b. Defendants Microsoft, Cisco and Comcast have posted false and misleading privacy policies and other false and misleading policies and representations at their respective web sites,
  - c. Defendant TRUSTe has conspired with Microsoft and Comcast to promote web site privacy policies and other policies which are false, contradictory, fraudulent, and/or misleading,
  - d. TRUSTe has engaged in a pattern and practice where TRUSTe tries to make it appear an entire company's privacy practices are covered by the TRUSTe requirements when only specific web sites within a company are covered by the TRUSTe requirements,
  - e. Defendants failed to honor their privacy policies that have provisions that would allow Plaintiff to review the profiles, Personally Identifiable Information (PII), and other information they collected about Plaintiff,
  - f. Defendant TRUSTe has operated a privacy policy verification service where they charged seal holders a fee to promote a privacy policy verification service which is fraudulent and meant to dupe Internet users and regulatory officials,
  - g. Defendant TRUSTe has operated a fraudulent dispute resolution service, and
  - h. Microsoft and Cisco have defamed Plaintiff by distributing false and misleading reports to third parties and labeled him a "spammer" causing Plaintiff's Internet mail communications to be repeatedly blocked.
2. This action seeks to recover damages and enjoin Defendants from engaging in various activities prohibited by law and/or contracts. In addition to enforcing contracts this action seeks relief under the

- a. New Jersey Consumer Fraud Act N.J.S.A 56:8-2 et seq.,
  - b. Electronic Communications Privacy Act [Federal Wiretap act, 18 U.S.C. § 2510, *et seq.* and Pen Register Act 18 U.S.C. § 2510, *et seq.*]
  - c. The New Jersey Wiretapping and Electronic Surveillance Control Act, N.J.S.A. 2A:156A-1, and/or
  - d. 47 USC Sec. 551 and 47 C.F.R. § 78.1716.
3. This action seeks to:
- a. Prohibit Microsoft, Cisco, and Comcast from eavesdropping on Plaintiff's Internet communications,
  - b. Prohibit all Defendants from disrupting the free market system and the system of "self-regulation" by posting privacy policies and other representations at their respective web sites that are false, misleading, and/or fraudulent,
  - c. Prohibit Microsoft from operating Internet Protocol (IP) address "blacklists" and distributing these "blacklists" to third parties without allowing the users of the IP addresses to review and correct the information collected that lead to the listing on "blacklists,"
  - d. Prohibit Cisco from operating Internet Protocol (IP) address "Reputation Scores" and publishing these "Reputation Scores" on the Internet without allowing the users of the IP addresses to review and correct the information collected that lead to the "Reputation Scores,"
  - e. Prohibit Microsoft and Cisco from further defaming Plaintiff by listing IP addresses used by Plaintiff on "blacklists" and giving IP addresses used by Plaintiff poor "Reputation Scores" and/or labeling Plaintiff as a "spammer" or making other similar accusations and representations.

- f. Prohibit Defendant TRUSTe from disrupting the free market system and the system of "self-regulation" by operating a fraudulent dispute resolution service for web site privacy policies,
- g. Prohibit TRUSTe from claiming entire companies or corporations are covered by the TRUSTe requirements when only specific web sites within a company are covered by the TRUSTe seal and associated requirements,
- h. Require Defendants to allow Plaintiff to review account, other information collected about him, Personally Identifiable Information (PII), and reports to third parties so Plaintiff may review and correct any incorrect or false information,
- i. Restrict Defendants from distributing information collected about Plaintiff to third parties in violation of posted privacy policies,
- j. Enforce the provisions of 47 USC Sec. 551 and 47 C.F.R. § 76.1716 for Plaintiff's account with Comcast so plaintiff may review his account information and prevent Comcast from distributing information about Plaintiff to third parties,
- k. Seek relief under the New Jersey Consumer Fraud Act N.J.S.A 56:8-2 et seq.,
- l. Collect compensatory damages,
- m. Collect punitive damages,
- n. Collect statutory damages pursuant to the federal Electronic Communications Privacy Act,
- o. Collect statutory damages under 47 USC Sec. 551 and 47 C.F.R. § 76.1716,

- p. Collect statutory damages pursuant to the New Jersey Wiretapping, and  
Electronic Surveillance Control Act.

**Plaintiff**

4. Plaintiff Russ Smith is a resident of Ocean City, N.J.
5. Plaintiff is a customer of Comcast for cable television and broadband Internet services.
6. Plaintiff is a customer of Microsoft and has purchased various software products such as operating systems.
7. Plaintiff has used the dispute resolution services offered by TRUSTe to attempt to resolve separate privacy policy disputes involving Microsoft and Comcast.
8. Plaintiff owns and operates a Limited Liability Company, The Keyword Factory, LLC (Keyword Factory) that operates web sites. Plaintiff has 100% ownership in Keyword Factory and no employees.
9. Plaintiff previously operated a Limited Liability Company in Virginia, The Consumer Information Organization, LLC doing business as Consumer.net, LLC (Consumer.net).
10. Plaintiff has testified and participated in various governmental proceedings involving privacy. These include:
  - a. Plaintiff made a presentation at the "Spam Summit" and Online Privacy workshop at the Federal Trade Commissions on or about 1998,
  - b. Plaintiff made a presentation at the "Do Not Call Forum" workshop operated by the Federal Trade Commissions in 2001 during the development of the National Do-Not-Call Registry (Exhibit A at footnote

- 21, Federal Register FTC Telemarketing Sales Rule, Proposed Rule.  
First 4 pages only of the notice are included for brevity).
- c. Plaintiff was recognized by the Federal Communications Commission (FCC) news release dated December 28, 1999 entitled "[FCC] Outlines Consumers' Rights to Prevent Telemarketing Calls." (Exhibit B).
11. Plaintiff has never been involved with knowingly sending unsolicited commercial e-mail, operating e-mailing lists, or sending large amounts of e-mail.
12. Plaintiff has held, since 2001, a professional certification in information systems security. Plaintiff is a Certified Information Systems Security Professional (CISSP) (Exhibit C) which is the largest certification program in the world related to computer security management. The CISSP program earned the ANSI ISO/IEC Standard 17024:2003 accreditation and is formally approved by the U.S. Department of Defense (DoD) in both their Information Assurance Technical (IAT) and Managerial (IAM) categories.
13. As a condition of CISSP certification Plaintiff must uphold the ISC2 Code of Ethics (Exhibit D) that requires Plaintiff to "Promote and preserve public trust and confidence in information and systems," "Preserve and strengthen the integrity of the public infrastructure," and "Discourage unsafe practice."
14. Plaintiff engages in political activities that include gathering information for the New Jersey Libertarian Party's Open Government Project (Exhibit E, Atlantic City Press article: *Ocean City agrees to provide public with copies of electronic documents*) and being a volunteer for the 2009 New Jersey gubernatorial primary election. Plaintiff also provides advice for sending e-

mail communications and newsletters to various political candidates and operatives.

15. Plaintiff has operated the web site [www.privacy.net](http://www.privacy.net) since 1999 that provides information and demonstrations about privacy to the general public.

Privacy.net and Plaintiff have been referenced by many national media outlets and Plaintiff has appeared on news programs Cable Network News (CNN) and Dateline NBC to discuss privacy. Privacy.net has been recommended by numerous sources such as:

- a. Consumer Reports in a 2003 article *Cover Your Tracks, Can Internet Washer Programs Keep Web Surfing Private?*, (Exhibit F)
- b. Kim Komando in her computer advice radio show and written articles such as the 2003 USAToday Article: *What Your IP Address Tells About You* (Exhibit G),
- c. ComputerWorld 2007 article: *How to surf anonymously without a trace* (Exhibit H), and
- d. The Malaysian Star 2007 article *Watch Your Step on the Web* (Exhibit I).

16. Plaintiff's personal and business activities and income depend on e-mail communications; the privacy, confidentiality, integrity, and availability of his home Internet communications; and his reputation for using the Internet in a responsible and legal manner.

17. Plaintiff relies on representations made at the web sites he visits.

**Defendant TRUSTe**

18. Defendant TRUSTe was misnamed in the suit and is True Ultimate Standards Everywhere, Inc. doing business as TRUSTe.

19. TRUSTe is:

- a. a not-for-profit corporation organized under the laws of California operating at 55 2nd Street, 2nd Floor San Francisco, CA 94105,
  - b. classified as a Section 501(c)(6) entity under the Internal Revenue Code,
  - c. doing business in New Jersey.
20. TRUSTe operates a web site at [www.truste.com](http://www.truste.com).
21. TRUSTe purports its mission to "*Build Trust Through Privacy*" and "*helps consumers and businesses identify trustworthy online organizations through its Web Privacy Seal ... resolves thousands of individual privacy disputes every year ...[by] promoting privacy policy disclosure, informed user consent, and consumer education ...[and] acts as an independent, unbiased trust entity.*" "*The TRUSTe privacy program – based on a branded online seal, the TRUSTe "trustmark" – bridges the gap between users' concerns over privacy and Web sites' needs for self-regulated information disclosure standards.*"  
(Exhibit J)
22. TRUSTe offers a privacy policy verification service for a fee and provides a TRUSTe license that permits the web site to display the TRUSTe "seal."
23. TRUSTe purports to offer services to "*Increase sales*", "*protect privacy and build customer confidence to work, play, and shop online.*" And offer an "*easy-to-use privacy dispute resolution service free to consumers*" (Exhibit K). TRUSTe claims their privacy services "*are Proven to Increase Conversions and Drive Revenue,*" (Exhibit L) "*help online businesses engender consumer trust that will be imperative in customer retention and acquisition... [s]how consumers that how you conduct business is fair and transparent with TRUSTe.*" (Exhibit M). TRUSTe also claims to work "*to advance privacy and*

*trust in a networked world," and that a benefit of the TRUSTe seal is to "Build trust and confidence by displaying trusted consumer-facing seals."* (Exhibit N)

24. The TRUSTe Watchdog dispute resolution service "allows consumers to report violations of posted privacy statements, or specific privacy concerns pertaining to TRUSTe member Web sites." (Exhibit O).
25. The purpose of Section IRC 501(c)(6) entities is to promote the common business interest and not to engage in a regular business of a kind ordinarily carried on for profit. Its activities are directed to the improvement of business conditions of one or more lines of business rather than the performance of particular services for individual persons. (Exhibit P)
26. TRUSTe's web site representations, including the documents "*Holding TRUSTe Members to Higher Online Privacy Standards*" (Exhibit Q) and TRUSTe privacy policy (Exhibit R) constitute a contract between TRUSTe and Plaintiff.
27. TRUSTe works with licensees to increase the sale of their products and services with the use of the TRUSTe "seal" and Watchdog dispute resolution service. These actions constitute the "sale or advertisement of merchandise" as defined under N.J.S.A 56:8-2.
28. TRUSTe offers their privacy seal to web sites for a fee. These actions constitute the "sale or advertisement of merchandise" as defined under N.J.S.A 56:8-2.

**Defendant Microsoft**

29. Defendant Microsoft Corporation ("Microsoft") was incorrectly named in the initial complaint as Microsoft, Inc. based on the registration with the State on

New Jersey under business ID 0100568573 with a registered agent at 830

Bear Tavern Rd., West Trenton, NJ 08628.

30. Microsoft is one of the largest computer software companies in the world offering products for sale such as computer operating systems and numerous other computer and Internet related services.
31. Microsoft offers a Frontbridge service that maintains IP address "blacklists" and uses and distributes these lists for the purposes of blocking e-mail communications.
32. Microsoft's sale of software to Plaintiff constitutes the "sale or advertisement of merchandise" as defined under N.J.S.A 56:8-2.
33. Microsoft's Frontbridge network and e-mail services constitutes the "sale or advertisement of merchandise" as defined under N.J.S.A 56:8-2.
34. Microsoft paid TRUSTe to have a seat on the TRUSTe Advisory Council (Exhibit S).
35. Microsoft Corporation is a TRUSTe licensee for its web sites.
36. Microsoft represents to the Federal Trade Commission in public comments about behavioral marketing and tracking consumers across different web sites that:
  - a. "*[Microsoft Corporation] abides by the standards set forth in ... the TRUSTe Privacy Program*" and that "*websites should be considered 'closely related' when a reasonable consumer would understand the sites are operated by the same entity.*" (Exhibit T, page 6 and footnote 11, attachments to letter not included).
37. Microsoft operates The "Frontbridge" services which compiles information about Internet mail servers by intercepting Internet e-mail traffic and creates

IP address "blacklists" or "blocklists" ("blacklists"). These blacklists are then distributed to third parties that use the Microsoft Frontbridge services for the purpose of blocking e-mail communications originating from the IP addresses on the blacklists.

38. In some cases Microsoft manages e-mail for clients and blocks e-mail communications originating from the IP addresses on the blacklists from reaching the client.

39. The Microsoft Frontbridge services are described at the web site <http://www.FrontBridge.com>. Users typing in [www.frontbridge.com](http://www.frontbridge.com) are redirected to the web page <http://www.microsoft.com/online/exchange-hosted-services.mspx> (Exhibit U). This web page contains a link to a "privacy statement" at <http://privacy.microsoft.com/en-us/default.mspx> which is endorsed by the TRUSTe privacy seal verification program. (Exhibit V)

40. The Microsoft privacy policy at <http://www.microsoft.com/online/exchange-hosted-services.mspx> constitutes a contract between Plaintiff and Microsoft.

41. Microsoft's privacy policy at <http://privacy.microsoft.com/en-us/fullnotice.mspx> #accessing states:

a. *"Accessing Your Personal Information ... You may have the ability to view or edit your personal information online ... Some Microsoft sites or services may collect personal information that is not accessible via the links above. However, in such cases, you may be able to access that information through alternative means of access described by the service. Or you can write us by using our Web form, and we will contact you within 30 days regarding your request."*

42. Microsoft has additional privacy policies that apply to the Frontbridge service at <http://www.frontbridge.com/legal/PrivacyStatement.htm> (Exhibit W) and <http://www.blueroomcreative.com/frontbridge/privacy.php> (Exhibit X) that also form a contractual relationship between Microsoft and Plaintiff.

**Defendant Comcast**

43. Defendant Comcast Cable Communications, LLC ("Comcast") has a business office at 341 West Ave, Ocean City, NJ and offers Broadband Internet services to millions of customers, including Plaintiff.

44. Defendant Comcast is one of the largest Internet Provider and Cable Television providers in the United States.

45. Plaintiff is a customer of Comcast and subscribes to Broadband Internet Services. These actions constitute the "sale or advertisement of merchandise" as defined under N.J.S.A 56:8-2.

46. On or about May 16, 2004 Plaintiff notified Comcast of the choice to "opt-out" of the binding arbitration clause added to the Comcast Subscriber Agreement. (Exhibit Y)

47. The Comcast Privacy Policy effective prior to October 6, 2009 which was found at <http://www.comcast.net/privacy/> was endorsed by the TRUSTe privacy seal (Exhibit Z) and states:

- a. *"We will not read your outgoing or incoming e-mail... We also monitor the performance of our Service and your Service connection in order to manage, maintain, and improve the Service and your connection to it. We (or our third party providers) use tools to help prevent and block "spam" e-mails, viruses, spyware, and other harmful or unwanted communications and programs on the Service. These tools may*

*automatically scan your e-mails ... and other files and communications in order to help us protect you and the Service against these harmful or unwanted communications and programs. However, these tools do not collect or disclose personally identifiable information about you..."*

48. The Comcast "2009 Comcast Customer Privacy Notice" found at

<http://www.comcast.com/customerprivacy/> which was part of the policy

endorsed by the TRUSTe privacy seal (Exhibit AA) prior to October 6, 2009 and states

- a. *"How can I see my personally identifiable information [PII] or CPNI and correct it, if necessary? You may examine and correct, if necessary, the personally identifiable information regarding you that is collected and maintained by Comcast in our regular business records."*

49. Comcast's Frequently Asked Questions about Network Management (Exhibit BB) states:

- a. *"Will the technique target ... applications, or make decisions about the content of my traffic?"*

*No. The new technique is "protocol-agnostic," which means that the system does not manage congestion based on the applications being used by customers. It is content neutral, so it does not depend on the type of content that is generating traffic congestion. Said another way, customer traffic is congestion-managed not based on their applications, but based on current network conditions and recent bytes transferred by users."*

50. Comcast's Agreement For Residential Services states (Exhibit CC)

- a. "... [Y]ou acknowledge and agree that Comcast and its agents have the right to monitor, from time to time, any such postings and transmissions, including without limitation e-mail,..."

51. Comcast's Help & Support Policy (Exhibit DD) states:

- a. "Port 25 is conduit on a computer that spammers can take control of and use to send their spam - often without the user ever knowing his/her computer has been 'hijacked'", and
- b. When spam from a compromised computer is detected, Comcast's anti-spam system automatically apply a sending block ..." and
- c. "Comcast works with our customers to block access to Port 25 and protect their PC. Comcast recommends that our customers establish a more secure email configuration on their PC - Port 587 - We have made it easy by creating a one-click fix that automatically configures your computers to this safer PC configuration."

52. Comcast's Acceptable Use Policy for High-Speed Internet Services states

(Exhibit EE):

- a. "... Comcast uses reasonable network management tools and techniques to protect customers from receiving spam and from sending spam (often without their knowledge over an infected computer)..." and
- b. "Comcast reserves the right to investigate suspected violations of this Policy, including the gathering of information from the user or users involved and the complaining party, if any, and examination of material

*on Comcast's servers and network. ... You expressly authorize and consent to Comcast and its suppliers cooperating with ... system administrators at other Internet service providers or other network or computing facilities in order to enforce this Policy."*

53. On October 6, 2009 Comcast changed its privacy policy at the Comcast.net web site (Exhibit FF). This change eliminated the TRUSTe privacy protection to cable subscribers.

54. Comcast's User Agreement, Comcast Privacy Policy at <http://www.comcast.net/privacy/>, 2009 Comcast Customer Privacy Notice, Network Management FAQ , Agreement For Residential Services, Help & Support Policy, and Acceptable Use Policy for High-Speed Internet Services form a contractual relationship between Comcast and Plaintiff and is an advertisement for goods and services as defined under the New Jersey Consumer Fraud Act N.J.S.A 56:8-2 et seq.

#### **Defendant CISCO**

55. Defendant Cisco Systems, Inc. ("Cisco") is registered with the State of New Jersey under business ID 0100437778 with a registered agent at 830 Bear Tavern Rd., West Trenton, NJ 08628.

56. Cisco is one of the largest suppliers of Internet-related computer hardware in the world. Many Cisco products are used for Internet communications.

57. Cisco operates a web site at [www.cisco.com](http://www.cisco.com). Cisco also operates other web sites such as [www.ironport.com](http://www.ironport.com) and [www.senderbase.org](http://www.senderbase.org).

58. Cisco operated and Ironport service that uses IP address "Reputations Scores" to block e-mail communications.

59. The Cisco Systems, Inc. Online Privacy Statement is found at

<http://cisco.com/web/siteassets/legal/privacy.html>. (exhibit GG) This policy states it does not apply to the subsidiary web site [www.ironport.com](http://www.ironport.com)

60. The Cisco Systems, Inc. Online Privacy Statement is found at

<http://cisco.com/web/siteassets/legal/privacy.html> applies to the subsidiary web site [www.senderbase.org](http://www.senderbase.org) and forms a contractual relationship between Cisco and Plaintiff.

61. [www.senderbase.org](http://www.senderbase.org) has a link entitled "Privacy Practices" that links to the Ironport privacy policy at <http://www.ironport.com/privacy/>. (Exhibit HH) This policy also forms a contractual relationship between Cisco and Plaintiff.

62. The Senderbase.org web site displays the IP address "Reputation Scores." (Exhibit II).

63. Cisco SenderBase service claims (Exhibits JJ and KK)

- a. To collect "*data on more than 25 percent of the world's email traffic*",
- b. To have "*the world's largest email and Web traffic monitoring service*",  
and
- c. the service can be used "*like a credit reporting service for email, providing comprehensive data that ISPs and companies can use to differentiate legitimate senders from spammers and other attackers and giving email administrators visibility into who is sending them email.*"

64. Cisco's SenderBase develops a "Reputation Score" for Internet IP addresses and publishes this "Reputation Score" to third parties using the [www.senderbase.org](http://www.senderbase.org) web site (Exhibit LL) and other methods.

#### **Plaintiff's Internet Connection and Email Configuration**

65. Plaintiff subscribes to the Comcast broadband Internet services. It is the only known residential broadband service available to Plaintiff in his area other than the Verizon services described below.

66. Plaintiff subscribes to the Verizon DSL Internet connection. This connection is generally not as fast as the Comcast broadband services but Plaintiff maintains this service when Comcast services are not available such as when Comcast disables portions of Plaintiff's service.

67. Plaintiff does not use e-mail services offered by either Comcast or Verizon.

68. Plaintiff operates his own e-mail services outside of the Comcast network.

69. Plaintiff's mail server is operated at IP address 64.251.31.213 at host name mail2.keywordfactory.com.

70. Plaintiff communicates with his email server using his home Internet connection and communicates via "Port 25," the standard for Internet e-mail.

71. The IP address 64.251.31.213 is Personally Identifiable Information (PII) because the information must be associated with a domain name and domain name registration which is publicly available.

72. Plaintiff's mail server maintains 2 accounts, one for Plaintiff and one for Plaintiff's Mother.

73. Plaintiff's Mother has never knowingly conducted any e-mail solicitation, mass e-mailing, using e-mailing lists or any other activity that involves sending a large amount of e-mail. Plaintiff's Mother does not have the expertise in Internet communications to conduct any mass e-mailings.

74. Plaintiff operates his own domain names used for e-mail.

75. Plaintiff uses "Sender Policy Framework" or SPF records for domains. (Exhibit MM) This system uses domain name records to prevent domain name

forgery or "spoofing" when e-mail is sent. In the case of the Plaintiff only one e-mail server is authorized to send e-mail for his domain names.

76. Microsoft recommends using SPF records to verify e-mail and uses the SPF procedure to verify e-mail senders. (Exhibit NN)

#### **Advice to Internet Industry by FCC and FTC**

77. Currently, federal agencies such as the Federal Communication Commission (FCC) and Federal Trade Commission (FTC) provide conflicting advice to the Internet industry as it relates to eavesdropping of Internet connections.

78. An FCC news release was issued August 1, 2008 meant to deter eavesdropping is entitled "**COMMISSION ORDERS COMCAST TO END DISCRIMINATORY NETWORK MANAGEMENT PRACTICES**" (Exhibit OO) and states:

- a. *"The Commission also concluded that Comcast's practices are not minimally intrusive, as the company claims, but rather are invasive and have significant effects. The Commission found that Comcast monitors its customers' connections using deep packet inspection and then determines how it will route some connections based not on their destinations but on their contents. In essence, Comcast opens its customers' mail because it wants to deliver mail not based on the address on the envelope but on the type of letter contained therein. The Commission also found that Comcast's conduct affected Internet users on a widespread basis. Indeed, Comcast may have interfered with up to three-quarters of all peer-to-peer connections in certain communities. The Commission concluded that the end result of Comcast's conduct was the blocking of Internet traffic, which had the effect of substantially"*

*impeding consumers' ability to access the content and to use the applications of their choice. The Commission noted that the record contained substantial evidence that customers, among other things, were unable to share music, watch video, or download software due to Comcast's misconduct."*

79. The FTC, on the other hand, has encouraged the Internet industry and Internet Service Providers, such as Comcast, to employ a series of techniques that monitor the content of Internet communications. In a letter from Comcast to Plaintiff on April 6, 2009 (Exhibit PP) Comcast points to FTC endorsement of eavesdropping techniques and other techniques that target certain Internet protocols and applications (Exhibit QQ<sup>1</sup>) such as:
- *block port 25 except for the outbound SMTP requirements of authenticated users of mail servers designed for client traffic. Explore implementing Authenticated SMTP on port 587 for clients who must operate outgoing mail servers.*
  - *apply rate-limiting controls for email relays.*
  - *identify computers that are sending atypical amounts of email, and take steps to determine if the computer is acting as a spam zombie. When necessary, quarantine the affected computer until the source of the problem is removed.*

---

<sup>1</sup> The page is a Google cache of the FTC page that had been removed from the Internet when Plaintiff tried to print the page.

80. The FTC also issued a "Spam Summit" report in November 2007 (Exhibit RR)

that recommends:

- a. "[to] urge ISP's to further implement negative scoring for non-authenticated email; and ... urge ISPs that have the ability to detect bot activity to stop bots immediately to prevent unauthorized access to consumers' computers by spammers and phishers."

81. In order to follow the FTC's guidance Internet Service Providers would be required to monitor, capture, and eavesdrop on Internet e-mail communications. For example, each of the methods below requires eavesdropping:

- a. "apply rate-limiting controls for email relays<sup>2</sup>,"
- b. "identify computers that are sending atypical amounts of email, and take steps to determine if the computer is acting as a spam zombie<sup>3</sup>,"
- c. "implement negative scoring for non-authenticated email<sup>4</sup>," and
- d. "detect bot activity to stop bots immediately<sup>5</sup>."

#### **Comcast's Policies not Enforceable by Comcast**

---

<sup>2</sup> To apply rate-limiting controls it is first necessary to monitor the communications and determine which communications are e-mail and attempt to determine whether the communications are authenticated.

<sup>3</sup> A "spam zombie" is a computer that is being controlled by someone else in order to send unsolicited e-mails without the owner's knowledge.

<sup>4</sup> In order to implement e-mail "scoring" the communications must be monitored and analyzed.

<sup>5</sup> A "bot" (or "robot") in this context is a computer that is being controlled by someone else sometimes without the owner's knowledge.

82. Comcast's policies concerning network management, security, and eavesdropping are so complicated that no reasonable person would be able to understand and comprehend them. Therefore, Comcast may not enforce these policies.

83. Comcast's policies concerning network management, security, and eavesdropping are contradictory and can not possibly be reconciled. Therefore, Comcast may not enforce these policies.

84. Comcast's policies concerning network management, security, and eavesdropping are meant to dupe federal regulatory authorities at the FTC and FCC as well as consumers. Different sets of policies were developed by Comcast to separately address FCC and FTC guidance that lead to the posting of policies that are contradictory and impossible to reconcile. Therefore, Comcast may not enforce these policies.

#### **Microsoft IP Address Blacklisting of Plaintiff**

85. On or about July 3, 2008 Microsoft included the IP address of Plaintiff's e-mail server in a "blacklist" distributed to third parties which resulted in the blocking of Plaintiff's e-mail communications. Exhibit SS is a reproduction of the notification Plaintiff received with e-mail subject and recipient address redacted.

86. On or about July 7, 2008 Microsoft communicated to Plaintiff (Exhibit TT):

- a. "...*Unfortunately we do not retain examples of the type of spam as evidence however we do keep logs of the sender/recipient information and the message ID and will be provided when the information is available. Unfortunately it is taking longer for us to provide this information as we are attempting to determine when this IP was first*

*listed on our blocklist. Our blocklisting system will not list an IP address unless there is a large volume of spam being captured for a domain."*

87. Microsoft did not provide Plaintiff any information that led to the blacklist

placement or any evidence of "spam" or associated logs.

88. Plaintiff spent approximately 4 hours checking his e-mail server configuration and logs and investigating Frontbridge.

89. Plaintiff reviewed several third party Internet postings that claimed Microsoft incorrectly blacklisted their IP addresses because they operated an e-mail server. Some posting appeared to be associates of law firms and not spammers. Plaintiff believed Microsoft either:

- a. Had a faulty method of blacklisting e-mail servers and/or
- b. Is engaged in anticompetitive behavior where Microsoft would blacklist those operating mail servers without subscribing to the Microsoft Frontbridge services.

90. On or about July 9, 2009 Plaintiff filed TRUSTe Watchdog Complaint #43304 against Microsoft.

91. TRUSTe responded on September 17, 2008 (Exhibit UU) :

*a. "...We have determined that the matter does not fall within the scope of our program. We are therefore unable to address your complaint. The link to the main Microsoft privacy policy is for the web site's marketing program. Users who sign up with the Frontbridge service are offered a different privacy policy (this works the same way for the Microsoft Office stand-alone program versus Office Online). TRUSTe*

*does not certify Frontbridge operations and we have no jurisdiction over this matter..."*

92. Plaintiff notified TRUSTe (Exhibit WW) that

- a. users blacklisted were directed to [www.frontbridge.com](http://www.frontbridge.com) which displays a link to the TRUSTe-endorsed privacy policy seal,
- b. those on the blacklist did not sign up for any Frontbridge service and were not bound by any contract other than what was displayed at the web site and that Plaintiff did not "sign up" for the Frontbridge service.

93. TRUSTe failed to prove a reasonable response that addressed issues or take reasonable action to ensure Microsoft complied with the TRUSTe program requirements.

94. Microsoft represents to the Federal Trade Commission in public comments that "*[Microsoft Corporation] abides by the standards set forth in ... the TRUSTe Privacy Program*" (Exhibit T, page 6, attachments to letter not included).

95. On or about September 23, 2008 Microsoft again placed Plaintiff on a blacklist that resulted in e-mail communications of Plaintiff being blocked and did not provide Plaintiff any information that led to the blacklist placement. Exhibit WW is a reproduction of the notification Plaintiff received with e-mail subject and recipient address redacted.

96. Plaintiff spent approximately an additional 1 hour checking the configurations of his mail sever.

97. TRUSTe contributed to the blocking of Plaintiff's e-mail by failing to require Microsoft to comply with their posted privacy policy. Microsoft never provided

Plaintiff with the information Microsoft had collected about Plaintiff so that Plaintiff could correct an errors and avoid future blocking.

**Comcast Blocking E-mail Communications of Plaintiff**

98. On or about March 9, 2009 Comcast blocked all outbound e-mail communications from Plaintiff's home Internet account.
99. Upon calling Comcast Plaintiff was told that Comcast detected "spam e-mail" coming from Plaintiff's account. Plaintiff asked Comcast to provide the evidence so Plaintiff could see what is wrong and fix it. Comcast refused and told Plaintiff the information was "proprietary." Plaintiff pointed to the Comcast privacy policy that states customers can review the information maintained in the account. Comcast told Plaintiff it didn't matter what the privacy policy said, the information was proprietary and Plaintiff wasn't getting it.
100. Comcast told Plaintiff they would unblock the e-mail port 25 this one time. Comcast would not tell Plaintiff why his e-mail communications was blocked. Comcast informed Plaintiff if similar activity was detected Plaintiff's e-mail communications would be permanently blocked unless Plaintiff paid for a higher level of service. Plaintiff was told he would not have to worry about any e-mail blocking if Plaintiff subscribed to a higher level of service.
101. Plaintiff spent approximately 8 hours checking configurations of his computers and scanning his scanning for virus and Trojan programs because Comcast would not explain why his account was flagged for security issues.
102. Plaintiff filed a TRUSTe Watchdog complaint number 48106 and sent a letter to the Comcast legal department. (Exhibit XX)

103.Comcast later claimed to Plaintiff in a letter dated April 6, 2009 (Exhibit PP) that the blocking was due to a report from a third party, IronPort, operated and owned by Cisco and a so-called IP address "reputation." Cisco later claimed another third party outside the United States, Spamhaus, actually made the report. Spamhaus web site claimed the "poor reputation" was based on spam originating from all of the Comcast networks and that: (Exhibit YY)

- a. All Comcast network addresses were given a poor reputation and
- b. No specific "spam e-mail" was detected from Plaintiff's Comcast account.

104.Such an explanation is absurd since this would result in all Comcast IP addresses being given the same poor reputation by Cisco and, therefore, Comcast would block all e-mail from all of its customers. This contradicts the Comcast's Help & Support Policy (Exhibit DD) that states the e-mail communications port 25 is not blocked by default.

105.On April 9, 2009 TRUSTe responded to Watchdog complaint number 48106 and stated (Exhibit ZZ):

- a. *"The Web site has cooperated with TRUSTe and has provided the information they used to base their service decision. The further issues you raise are outside the scope of TRUSTe's privacy program."*

106.Plaaintiff complained to TRUSTe that the responses received from Comcast and their posted policies were contradictory (Exhibit AAA). TRUSTe failed to

provide a reasonable response that addressed issues or take reasonable action to ensure Comcast complied with the TRUSTe program requirements.

107. On or about April 16, 2009 Comcast again blocked all outbound communications of Plaintiff and told Plaintiff more "spam" e-mail was detected coming from his computer.

108. Plaintiff spent approximately 1 additional hour checking configurations of his computers and scanning his scanning for virus and Trojan.

109. Plaintiff has requested Comcast allow Plaintiff review his account information pursuant to 47 USC Sec. 551 and 47 C.F.R. § 76.1716. Comcast has not permitted Plaintiff to access his account information (with the exception of invoices). Comcast's attorney Monica Mosley, demanded Plaintiff provide a reason for the requested account information. Plaintiff stated he wanted to see the notations on his account that caused his e-mail communications to be blocked and notifications that could cause future "permanent" blocking of Plaintiff's e-mail communications. Comcast's attorney Monica Moseley then denied the request.

110. TRUSTe contributed to the blocking of Plaintiff's e-mail communications by failing to require Comcast to comply with their posted privacy policy. Microsoft never provided Plaintiff with the information Microsoft had collected about Plaintiff so that Plaintiff could correct an errors and avoid future blocking.

111. TRUSTe has intentionally deceived the public (including the Plaintiff) by making false representations at its web site (Exhibit BBB) by claiming "TRUSTe certifies ... the Comcast ... privacy statements ..." when TRUSTe only certifies privacy policies of some specific Comcast web sites . TRUSTe

has continued to make this representation after October 6, 2009 when Comcast removed all cable, Internet, and phone subscribers' privacy policies from the TRUSTe program. Comcast moved the privacy policies of these subscribers to Comcast.com web site which is not licensed by TRUSTe.

(Exhibit FF)

**Cisco Fraudulently Operating E-mail "Credit" Reporting Service**

112.Cisco claims to operate a Credit Reporting Service for e-mail and develops a "reputation" score for Internet IP addresses and reports and publishes this information to third parties.

113.A reasonable person would expect that when an entity claims to be operating a service that is, or is similar to, a "credit reporting service" that those listed in the reports would be able to obtain the reports and dispute any information contained in the reports.

114.Cisco's privacy policy states: "*Accessing and updating your personal information[:] We need your help in keeping the Personal Information you have shared with us accurate and up to date. Please notify us of any changes to your Personal Information.*"

115.Cisco told Plaintiff that they monitor Internet traffic in many networks across the world to develop a "Reputation Scores" for IP addresses.

116.Plaintiff made several requests to Cisco to obtain the information they collected to produce a "Reputation Score" about Plaintiff's Internet connection IP address.

117.Cisco pointed Plaintiff to a "reputation" web page at SenderBase.org that claimed the "reputation" score was actually taken from another third party in the United Kingdom, Spamhaus. Spamhaus web site claimed the "poor

reputation" was based on spam originating from all of the Comcast networks and that all Comcast network addresses were given a poor reputation and that no specific "spam e-mail" was detected from Plaintiff's Comcast account.

#### **Defendants Further Violations of Privacy Policies**

118. On information and belief all Defendants have violated their respective privacy policies by distributing information about Plaintiff as a result of his complaints and in the conduct of legal proceedings.

119. Comcast's privacy policy prevents distribution of personal information except when required by law. Both Microsoft and Comcast are prohibited from distribution of personal information unless "necessary." Answering a civil complaint is not required by law and not "necessary" making such distributions prohibited.

120. Comcast distributed Plaintiff's home address in court papers and filed such in the Pacer feder court document system. Comcast refused to redact this information upon request and pursuant to the Comcast privacy policy and 47 USC Sec. 551 and 47 C.F.R. § 76.1716. Plaintiff filed TRUSTe Watchdog complaint number 55899 as a result of this incident.

#### **Counts - TRUSTe**

121. TRUSTe made false and misleading representations at its web site in violation of the New Jersey Consumer Fraud Act and/or has failed to comply with its contractual requirements to offer a dispute resolution service causing harm to Plaintiff by:

- a. **Count 1:** failing to provide a reasonable resolution to complaint filed by Plaintiff against Microsoft,
- b. **Count 2:** failing to remove Microsoft from the TRUSTe program after being aware of non-compliance with the program requirements,
- c. **Count 3:** failing to take reasonable action after being aware Microsoft posted fraudulent or misleading privacy policy and other representations at their web sites,
- d. **Count 4:** failing to take reasonable action after being aware Microsoft did not allow Plaintiff to have access to the PII Microsoft collected about Plaintiff,
- e. **Count 5:** failing to take reasonable action after being aware Microsoft did not allow Plaintiff to correct the PII Microsoft has collected about Plaintiff,
- f. **Count 6:** failing to provide a reasonable resolution to complaint filed by Plaintiff against Comcast,
- g. **Count 7:** failing to remove Comcast from the TRUSTe program after being aware of non-compliance with the program requirements,
- h. **Count 8:** failing to take reasonable action after being aware Comcast posted fraudulent or misleading privacy policy and other representations at their web sites,
- i. **Count 9:** failing to take reasonable action after being aware Comcast did not allow Plaintiff to have access to the PII and other information Comcast collected about Plaintiff,

- j. **Count 10:** failing to take reasonable action after being aware Comcast did not allow Plaintiff to correct the PII Comcast has collected about Plaintiff,
- k. **Count 11:** failing to take reasonable action after being aware Comcast continued to distribute PII about Plaintiff in court proceedings, and
- l. **Count 12:** making false representations at its web site by claiming TRUSTe certifies Comcast privacy policies when it only certifies some of their web sites.

#### **Counts - Comcast**

**122.Count 13:** Comcast violated the New Jersey Wiretapping and Electronic Surveillance Control Act [N.J.S.A 2A:156A-1] and caused harm to Plaintiff by monitoring Plaintiff's Internet communications and/or allowing third parties to do so.

**123.Count 14:** Comcast violated the Federal Wiretap Law [18 USC § 2510 et seq.] and caused harm to Plaintiff by monitoring Plaintiff's Internet communications and/or allowing third parties to do so.

**124.Count 15:** Comcast violated the Pen Register Act [18 USC § 3121 et seq.] by monitoring Plaintiff's Internet communications and/or allowing third parties to do so.

**125.**Comcast made false and misleading representations in violation of the New Jersey Consumer Fraud Act and/or has failed to comply with its contractual agreements and caused harm to Plaintiff by:

- a. **Count 16:** not providing Plaintiff access the PII Comcast compiled about Plaintiff,
- b. **Count 17:** not allowing Plaintiff to correct the PII Comcast has collected about Plaintiff,
- c. **Count 18:** providing a false and/or misleading explanation of why Plaintiff's e-mail communications were blocked,
- d. **Count 19:** monitoring and blocking specific protocols and services, such as e-mail, while making the representation that monitoring and blocking is "protocol agnostic," and
- e. **Count 20:** posting various policies at its web site which are inconstant about how Internet communications are monitored and/or blocked,
- f. **Count 21:** not allowing Plaintiff access the PII they compiled about Plaintiff as a result of violating its agreement with the City of Ocean City, NJ
- g. **Count 22:** not allowing Plaintiff access his account information in violation of the Cable Communications Policy Act of 1984, 47 USC Sec. 551 and 47 C.F.R. § 76.1716, and
- h. **Count 23:** not distributing Plaintiff PII to third parties and to the Court in violation of the Cable Communications Policy Act of 1984, 47 USC Sec. 551 and 47 C.F.R. § 76.1718.

#### **Counts - Microsoft**

126. **Count 24:** Microsoft violated the Federal Wiretap Law [18 USC § 2510 et seq.] and caused harm to Plaintiff by monitoring Plaintiff's Internet communications.

127. **Count 25:** Microsoft violated the Pen Register Act [18 USC § 3121 et seq.] and caused harm to Plaintiff by monitoring Plaintiff's Internet communications.

128. Microsoft made false and misleading representations in violation of the New Jersey Consumer Fraud Act and/or has failed to comply with its contractual agreements and caused harm to Plaintiff by:

- a. **Count 26:** claiming the Microsoft Privacy Policy does not apply to their Frontbridge Service and caused harm to Plaintiff by:
  - i. redirecting Internet users who typed in www.FrontBridge.com to a web page at Microsoft.com, and then
  - ii. claiming that the Microsoft privacy policy does not apply to the Frontbridge service and/or www.FrontBridge.com while claiming the opposite in public comments made to the Federal Trade Commission.
- b. **Count 27:** not providing Plaintiff access the PII Microsoft compiled about Plaintiff.
- c. **Count 28:** not allowing Plaintiff to correct the PII Microsoft has collected about Plaintiff, and
- d. **Count 29:** not following through with a promise to Plaintiff to send PII and/or e-mail logs Microsoft has collected about Plaintiff.
- e. **Count 30:** defaming Plaintiff by placing his IP address on blacklists/blocklists for e-mail communications without allowing

Plaintiff to review and correct, if necessary, the information that led to these blacklist/blocklist listings.

#### **Counts - Cisco**

129. Cisco made false and misleading representations in violation of the New Jersey Consumer Fraud Act and/or has failed to comply with its contractual agreements and caused harm to Plaintiff by:

- a. **Count 31:** not providing Plaintiff access the PII Cisco compiled about Plaintiff,
- b. **Count 32:** not allowing Plaintiff to correct the PII Cisco collected about Plaintiff,
- c. **Count 33:** not following through with a promise to Plaintiff to send PII Cisco has collected about Plaintiff,
- d. **Count 34:** claiming Spamhaus was responsible for the poor reputation score of Plaintiff's IP address, and
- e. **Count 35:** falsely advertising their Ironport service as being like a credit reporting service for e-mail.

130. **Count 36:** Cisco violated the New Jersey Wiretapping and Electronic Surveillance Control Act [N.J.S.A 2A:156A-1] and caused harm to Plaintiff by monitoring Plaintiff's Internet communications and/or allowing third parties to do so.

131. **Count 37:** Cisco violated the Federal Wiretap Law [18 USC § 2510 et seq.] by monitoring Plaintiff's Internet communications and/or allowing third parties to do so and caused harm to Plaintiff.

**132.Count 38:** Cisco violated the Pen Register Act [18 USC § 3121 et seq.] by monitoring Plaintiff's Internet communications and/or allowing third parties to do so and caused harm to Plaintiff.

**133.Count 39:** Cisco caused harm to Plaintiff by defaming Plaintiff by giving a "Reputation Score" for e-mail communications to the IP address used by Plaintiff without allowing Plaintiff to review and correct, if necessary, the information that led to the reputation score.

#### **Relief Sought**

**134.The following relief is sought<sup>6</sup>:**

- a. Prohibit Microsoft, Comcast and Cisco from eavesdropping on Internet communications of the citizens of New Jersey,
- b. Prohibit Comcast displaying or distributing false or misleading portions of the Privacy Policy, Customer Privacy Notice, Acceptable Use Policy for High-Speed Internet Services, Network Management Policy, Network Management FAQ, Spam Policy and other related information to the citizens of New Jersey,
- c. Prohibit Microsoft from displaying or distributing false or misleading portions of the Privacy Statement and other related information to the citizens of New Jersey,

---

<sup>6</sup> Some of the damages requested are for small amounts of money which may be "identifiable trifles." Courts have held that an identifiable trifle is enough for standing to fight out a question of principle. (see Bell v Acxiom 2006 WL 2850042 (E.D. Ark. Oct 3, 2006) (Exhibit CCC). In this Complaint Plaintiff wishes to be free from the eavesdropping of his Internet connection and be free to conduct his activities without having his communications disrupted or being defamed.

- d. Prohibit Cisco from displaying or distributing false or misleading portions of the Privacy Statement and other related information to the citizens of New Jersey,
- e. Prohibit TRUSTe from conducting a false or misleading dispute resolutions services to the citizens of New Jersey,
- f. Prohibit TRUSTe from endorsing any privacy policies displayed to citizens of New Jersey,
- g. Prohibit TRUSTe from claiming they certify entire companies when they only certify specific web sites,
- h. Require Microsoft, Comcast and Cisco to provide Plaintiff with all information collected about Plaintiff's Internet communications or any associated data or any PII and allow Plaintiff to correct any erroneous information, and
- i. Prohibit Microsoft, Comcast and Cisco from distributing any defamatory information about Plaintiff to any third party,
- j. Compensatory damages to compensate Plaintiff for being unable to communicate via e-mail without disruptions,
- k. Compensatory damages to compensate Plaintiff for being unable to communicate via e-mail without eavesdropping,
- l. Compensatory damages to compensate Plaintiff for being unable to correct "profiles" maintained by Defendants about Plaintiff,
- m. Compensatory damages to compensate Plaintiff for damaging his reputation,
- n. Compensatory damages to compensate Plaintiff for past or future loss of earnings,

- o. Compensatory damages to compensate Plaintiff for time lost in running his business,
- p. Treble compensatory damages and legal fees pursuant to the New Jersey Consumer Fraud Act,
- q. Punitive damages for violating Plaintiff's privacy,
- r. Punitive damages for damaging Plaintiff's reputation
- s. Statutory damages pursuant to the Electronic Communications Privacy Act,
- t. Statutory damages pursuant to The New Jersey Wiretapping and Electronic Surveillance Control Act
- u. Statutory damages pursuant to 47 USC Sec. 551 and 47 C.F.R. § 76.1716,
- v. Costs of this action, and
- w. Any other action the Court deems just and equitable.



Russ Smith, pro se  
October 8, 2009

#### CERTIFICATION OF NO OTHER ACTIONS

I certify that the dispute about which I am suing is not the subject of any other action pending in any other court or a pending arbitration proceeding to the best of my knowledge and belief. Also, to the best of my knowledge and belief no other action or arbitration proceeding is contemplated. Further, other than the parties set forth in this complaint, I know of no other parties that should be made a part of this lawsuit. In addition, I recognize my continuing obligation to file and serve on all parties and the court an amended certification if there is a change in the facts stated in this original certification.

Dated: 10/8/2009 Signature: Russ Smith